

351.7232 Montana.
L72mcp Legislature.
1987 Office of the
Legislative
Auditor
Microcomputer
controls 5/55

State of Montana
Office of the Legislative Auditor

PERFORMANCE AUDIT

MICROCOMPUTER CONTROLS

This report contains recommendations for developing guidelines for formulating effective microcomputer controls. The recommendations concern:

- Developing guidelines for organizational controls.
- Involving agency data processing personnel in microcomputer acquisition and installation.
- Developing guidelines for access controls for microcomputer systems.
- Developing guidelines for documentation of micro-computer applications.
- Developing guidelines for ownership rights and licensing agreements for microcomputer software.

PLEASE RETURN



Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
Helena, Montana 59620

STATE DOCUMENTS DIVISION

APR 28 1988

MONTANA STATE LIBRARY
1515 E. 6th AVE.
HELENA, MONTANA 59620



PERFORMANCE AUDITS

Performance audits conducted by the Office of the Legislative Auditor are designed to assess state government operations. From the audit work, a determination is made as to whether agencies and programs are accomplishing their purposes, and whether they can do so with greater efficiency and economy. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the performance audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration, statistics, economics, computer science, and engineering.

Performance audits are performed at the request of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

LEGISLATIVE AUDIT COMMITTEE

Senator Judy Jacobson, Chairman

Senator Delwyn Gage

Senator Tom Keating

Senator Ted Neuman

Representative John Cobb, Vice Chairman

Representative Dorothy Bradley

Representative Harry Fritz

Representative Bruce Simon

AUG 23 1988

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
HELENA, MONTANA 59620
406/444-3122



SCOTT A. SEACAT
LEGISLATIVE AUDITOR

March 1988

DEPUTY LEGISLATIVE AUDITORS:

JAMES GILLET
FINANCIAL COMPLIANCE AUDITS

JIM PELLEGRINI
PERFORMANCE AUDITS

LEGAL COUNSEL:

JOHN W. NORTHEY

The Legislative Audit Committee
of the Montana State Legislature:

This is our performance audit of state agency controls over micro-computers.

This report contains recommendations concerning the establishment of guidelines for the development of microcomputer controls. Responses from the Information Services Division of the Department of Administration are contained at the end of the report.

We wish to express our appreciation to the staff of all the agencies we visited for their cooperation and assistance.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Scott A. Seacat", written over a horizontal line.
Scott A. Seacat
Legislative Auditor

PERFORMANCE AUDIT REPORT
MICROCOMPUTER CONTROLS

March 1988

Report Number 87P-36

Members of the audit staff involved in this audit were Jim Pellegrini, Rob Spear, and Jerry Kozak. Additional information on the audit can be obtained by contacting the Office of the Legislative Auditor at (406) 444-3122.

TABLE OF CONTENTS

	<u>Page</u>
List of Illustrations	iii
Administrative Officials	iv

CHAPTER I INTRODUCTION

Scope of Audit	1
Compliance	2
Future Audit Work	2

CHAPTER II BACKGROUND

Microcomputer Expansion	3
Microcomputer Uses	4
Microcomputer Configurations	4
Microcomputer Acquisition	5
Microcomputer Management	6

CHAPTER III MICROCOMPUTER CONTROLS

Control Weaknesses	8
Organizational Controls	11
Needs Analysis	12
Hardware and Software Inventories	12
Training	12
Maintenance	13

TABLE OF CONTENTS
(Continued)

	<u>Page</u>
Data Processing Personnel	14
Conclusion	14
Access and Security Controls	15
Physical Access	15
Logical Access	16
Backup and Disaster Recovery	16
Conclusion	17
Documentation	17
Software Licensing and Ownership	18
Software Licensing Agreements	18
Ownership Rights	19
Summary	19
Agency Response	20

LIST OF ILLUSTRATIONS

<u>No.</u>		<u>Page</u>
1.	Number of Microcomputers in State Government	4
2.	Agency Microcomputer Controls Summary	10

ADMINISTRATIVE OFFICIALS

Department of Administration

Ellen Feaver, Director

Dave Ashley, Deputy Director

Information Services Division

Mike Trevor, Administrator

CHAPTER I

INTRODUCTION

At the request of the Legislative Audit Committee, a performance audit was conducted of the state's acquisition, use, and control of microcomputers.

The objectives of our performance audit were:

1. To gather information on microcomputer equipment statewide and determine the extent of hardware and software inventories.
2. To determine the process used by agencies in the acquisition of microcomputers.
3. To identify "high risk" or important microcomputer applications used by state agencies.
4. To determine the adequacy of controls over microcomputer systems.

SCOPE OF AUDIT

The audit was conducted in accordance with generally accepted governmental performance auditing standards. Formal audit work focused on microcomputer controls at state agencies selected through an initial risk assessment of all state agencies. Risk factors considered were: the number of microcomputers in each agency, total dollar amount invested in microcomputers and peripherals (printers, modems, etc.), existence of agency microcomputer policies and procedures, training of personnel, and the number of authorized people signing purchase orders.

During our initial review we found similar audit issues were developing. Consequently, our audit scope was reduced to review microcomputer operations at five departments: the Department of Health and Environmental Sciences; the Department of Highways; the Department of Fish, Wildlife and Parks; the Department of Revenue; and the Department of Social and Rehabilitation Services. These departments own approximately 30 percent of state government's microcomputers (excluding university systems). We did not include the university system in our audit as originally planned.

We discussed our preliminary findings with management personnel from the Information Services Division of the Department of Administration. Since then the division has developed some preliminary guidelines for microcomputer management.

Audit memorandums were sent to each audited agency after our review was completed, communicating specific findings to agency personnel.

COMPLIANCE

As part of our audit we reviewed compliance with laws, administrative rules, and Montana Operations Manual policies regarding the acquisition and security of microcomputers. No significant instances of noncompliance were found during our audit. For items we did not specifically test for compliance, nothing came to our attention that would indicate instances of noncompliance.

FUTURE AUDIT WORK

During our audit we reviewed general and application controls over agency microcomputers. We did not do an in-depth analysis of all microcomputer applications in each agency. However, we did test several spreadsheet applications during the audit and found the information being produced was reliable.

In the course of future audit work (financial-compliance audits, performance audits) we will continue to review general and application controls. According to Standards for Audit of Governmental Organizations, Programs, Activities, and Functions, the auditors shall:

1. Review general controls in data processing systems to determine whether: (a) the controls have been designed according to management direction and known legal requirements, and (b) the controls are operating effectively to provide reliability of, and security over, the data being processed.
2. Review application controls of installed data processing applications upon which the auditor is relying to assess their reliability in processing data in a timely, accurate, and complete manner.

CHAPTER II

BACKGROUND

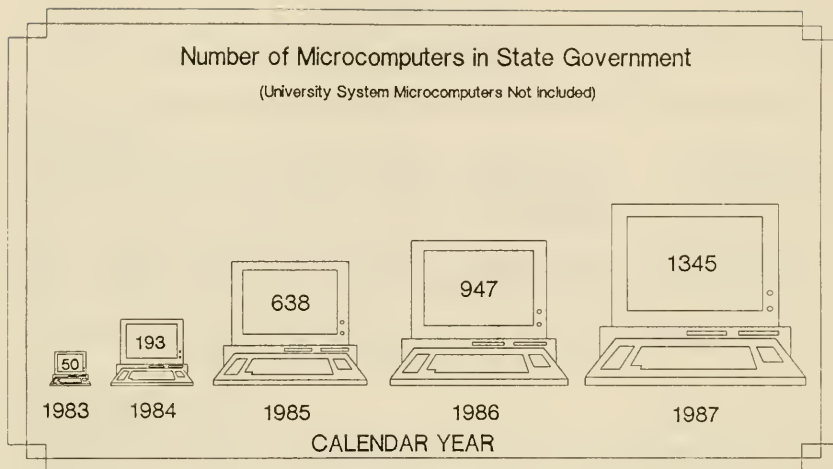
There are three types of computers being used in state government:

- | | |
|---------------|--|
| Mainframe | Large capacity computer capable of running a variety of system software with sizeable storage and output capabilities. |
| Minicomputer | Smaller version of the mainframe with a smaller storage capacity dedicated to a limited number of applications. |
| Microcomputer | Desk-sized processor used for a limited set of functions. Less storage capacity than the minicomputer. |

This chapter provides an overview of state government use of microcomputer hardware (equipment used in the microcomputer operation) and software (computer programs used in the microcomputer operation). It outlines the different configurations available for microcomputers and gives a brief explanation of what microcomputers are used for in state government. It also explains the acquisition process used by agencies when acquiring microcomputer equipment.

MICROCOMPUTER EXPANSION

According to figures obtained on microcomputer acquisition since 1983 (see Illustration I), there are approximately 1,345 microcomputers in state government (over 1,700 more are in the university system). This has resulted in an investment estimated at over \$7.5 million, not including microcomputer peripherals (i.e printers, etc.)



Source: Compiled by the Office of the Legislative Auditor from Information Services Division records.

Illustration 1

Microcomputer Uses

Microcomputers are serving state government in a variety of different ways. Currently the most common use for microcomputers is word processing. Microcomputers now replace larger word processing units. Spreadsheet applications are developed on microcomputers; aiding agencies in projection of budgets, development of financial schedules, and day-to-day analysis. Data base applications assist agencies in sharing information and in monitoring different programs. Graphics packages allow agencies to convert management information into charts and graphs. Microcomputers also perform some work previously done on the state's larger mainframe computers. Because microcomputers are used as mainframe terminals, the acquisition of mainframe terminals decreased from 314 in 1984 to just 34 in 1987.

Microcomputer Configurations

There are basically three ways microcomputer systems are used in state government. The first configuration is a stand-alone microcomputer system. A

stand-alone microcomputer system is designed to operate as an independent processing unit. It is not attached to other processing units and is equipped with its own hardware and applications software.

A second configuration is the local area network (LAN). The LAN is a communication network allowing two or more microcomputers to share resources with one another. The LAN offers several advantages for the user. Data can be transferred faster resulting in productivity gains, the need for control is increased because microcomputers are linked together by a central processing facility, and overall cost of the system can be reduced because expensive peripherals, such as printers, can be shared.

Finally, stand-alone microcomputers and networked microcomputers can be linked to the state data network. The microcomputer can be used as a terminal which allows it to perform the same functions as a regular mainframe terminal. It can also be used to transfer data to and from the mainframe for storage and processing.

MICROCOMPUTER ACQUISITION

Agencies may follow one of two courses of action in obtaining microcomputers. An agency may purchase a microcomputer off the state term contract or elect to go out for bid. A term contract is a contract for a specific item competitively bid by the Purchasing Bureau for the state. The successful bidder has the right to sell that item to a department or agency for a certain period of time at a set price. Only specific brands are available to an agency purchasing a microcomputer off a term contract. Agencies are not required to purchase off the term contract because in some cases an agency may want a different brand of microcomputer than what is available on the term contract.

Section 2-17-501, MCA, requires approval for the purchase of microcomputer equipment from the Information Services Division of the Department of Administration. As part of the approval process the Information Services Division (ISD) reviews requisitions for consistency with ISD's long range plans ensuring compatibility of equipment.

MICROCOMPUTER MANAGEMENT

The management of microcomputer systems varies between departments. Some departments have established a microcomputer support function providing all hardware and software maintenance, as well as problem resolution. Other departments have assigned one individual in each division to monitor the use of microcomputers and provide needed support. In one agency we found one person was responsible for providing support to the entire department.

Several of the agencies we reviewed had steering committees responsible for reviewing and approving requisitions for microcomputer acquisition. Steering committees aid agencies in ensuring criteria for acquisition is being met and compatibility of hardware and software is being realized between programs within the department.

Microcomputer support is available from the Information Services Division. The division offers assistance in three ways for software they support. An agency may participate in a full subscription program: paying a fixed monthly fee that is negotiated depending on the total number of microcomputers an agency may have. This subscription entitles an agency to unlimited on-site support and problem resolution, unlimited use of Disoss (electronic mail) and Personal Manager (calendering), a discount for microcomputer training classes, equipment pool discounts, and minor application development assistance. Another ISD subscription option is the individual personal computer and terminal subscription program. Under this alternative an agency pays twenty dollars per month to subscribe an individual computer for Information Center support. The agency receives unlimited assistance for that microcomputer, unlimited use of Disoss and Personal Manager and training discounts to electronic mail and calendering courses. The third option is no subscription. For agencies that do not subscribe, free telephone assistance will be available for up to two hours. Any assistance from the Information Center beyond two hours will be billed at thirty-two dollars an hour.

Two other state government groups are involved in agency management of data processing: the Data Processing Advisory Council and the Data Processing Managers Group. The Data Processing Advisory Council was established in 1979 by section 2-17-502, MCA. Council members are selected by the director of the Department of Administration and currently includes twenty-one department directors or deputy directors, including the Legislative

Auditor. The goals of the council are to educate agencies on the appropriate use of computers and make recommendations on:

- establishment of a planning process to provide management direction to the information processing effort;
- establishment of policies to assure efficient utilization of information processing resources;
- strategies to manage information resources more effectively; and
- coordination of the rapid expansion of office automation throughout state government.

The Data Processing Managers Group was informally established in 1978. Ten data processing management personnel from various state agencies, including a representative from the Legislative Auditor's Office, make up the group. The group was organized to review and make recommendations on data processing issues affecting state government data processing activities. The group participates in the statewide data processing planning effort by interacting with agency data processing programs.

CHAPTER III

MICROCOMPUTER CONTROLS

Since microcomputer technology is expanding and becoming more sophisticated, it is becoming increasingly important to manage and protect the state's investment in microcomputers. One way of addressing this need is through the development of microcomputer controls.

CONTROL WEAKNESSES

There are four major risks inherent in microcomputer systems: hardware, software, network, and user-related risks. For example; microcomputer hardware is usually lightweight and easily portable. Pocket size diskettes are easy to remove and provide easy access to information. On most microcomputers there is no password protection over access to users' files. Files can be erased, causing loss of data. Documentation and testing for microcomputer spreadsheet programs, which are used for decision making, is often neglected. Networking microcomputers together increases exposure of access by unauthorized persons. Finally, there is failure by agency microcomputer users to employ backup and control procedures.

As the configurations for microcomputers become more complex so should the controls over the configurations themselves. For example, stand-alone machines are usually the responsibility of one individual and strong physical access controls should exist. As microcomputers are networked, agencies should become more concerned with not only physical access controls, but with access controls over the information and software being stored on the networked system. Additionally, once microcomputers are allowed to access a mainframe the issue of security over mainframe information becomes a concern. Most of the data stored on the state's mainframe is subject to an Access Control Facility (ACF2) password protection application. Once information is transferred to the microcomputer ACF2 protection is lost and security becomes the responsibility of the microcomputer user.

During our audit work we evaluated the adequacy of microcomputer controls in each of five agencies. We found several agency-wide weaknesses which we attribute to a lack of such controls.

State law, section 2-17-501, MCA, provides, " ... the director of the Department of Administration shall establish policies and a statewide plan, in cooperation with state agencies, for the operation and development of data processing for state government...." The Information Services Division has developed guidelines in the form of the Montana Operations Manual (MOM). The Montana Operations Manual provides agencies with guidelines for mainframe computer hardware and software acquisition and use. Although the concepts may apply to microcomputers, the guidelines are not specific to microcomputer use.

Section 2-15-114, MCA, provides, "each department head is responsible for assuring an adequate level of security for all data and information technology resources within his department...."

We believe the Information Services Division could work together with the Data Processing Advisory Council and the Data Processing Managers Group to establish more specific guidelines for effective microcomputer controls. Once guidelines are developed it would then be the responsibility of each department director to establish, document and enforce microcomputer controls.

The agency-wide microcomputer control weaknesses we noted are summarized in the following chart. The types of controls listed in the chart are basic and provide for safeguarding of assets, confidentiality of information, efficient operations, and effective use of agency resources. As illustrated by the overall column, a majority of the agencies we audited had weaknesses in almost all controls tested.

AGENCY MICROCOMPUTER CONTROLS SUMMARY

S = STRENGTH

W = WEAKNESS

AGENCY
#1 #2 #3 #4 #5 OVERALL

ORGANIZATIONAL CONTROLS

Needs Analysis	W	W	S	S	W	W
Hardware Inventories	S	S	W	W	S	S
Software Inventories	S	S	W	W	W	W
Maintenance	W	W	S	S	W	W
Training	W	W	W	S	S	W
Policies & Procedures	W	W	W	S	W	W

ACCESS & SECURITY CONTROLS

Physical Access						
Hardware	S	S	S	S	S	S
Software & Diskettes	W	W	W	W	W	W
Logical Access	W	S	S	W	W	W
Backups	W	W	W	S	S	W
Disaster Recovery	W	W	W	S	S	W

OTHER CONTROLS

Documentation	W	W	W	W	W	W
Copyright Laws	W	S	W	S	W	W
Ownership Rights	W	W	W	W	W	W

Source: Compiled by the Office of the Legislative Auditor

Illustration 2

Based upon weaknesses found with agency microcomputer controls the following sections contain recommendations relating to organizational controls (controls which establish control over microcomputer operations), access and security controls (controls that provide adequate security over hardware and software), documentation (written support explaining how applications function), software ownership rights, and software licensing agreements.

ORGANIZATIONAL CONTROLS

As part of our audit work we examined organizational controls over microcomputers in the five agencies we reviewed. Responsibility for implementing these controls ranged from one person to an entire support section.

Proper organizational controls provide for:

- Some type of needs analysis study for microcomputer hardware and software acquisitions to ensure cost/effective and coordinated purchases;
- Clear lines of authority so microcomputer users know who to contact for support;
- Adequate hardware and software inventories to control assets;
- Microcomputer maintenance programs to ensure continued operations;
- Sufficient training for microcomputer users to provide for more efficient and effective use of resources; and
- Adequate policies and procedures to properly communicate the control objectives.

The following sections discuss the weaknesses we found in agency organizational controls.

Needs Analysis

We noted three of the five agencies reviewed were not performing adequate needs analysis studies prior to microcomputer acquisition. As a result, agencies purchased hardware and software and then planned where equipment should be placed, rather than determining what equipment needs

were and then purchasing the microcomputers. We also found agencies were purchasing software not supported by the Information Services Division even though the supported software would perform the same function.

Proper needs analyses are a significant part of planning designed to aid an agency in determining:

- if sufficient funding is available to acquire and maintain equipment;
- a cost/benefit of the considered equipment;
- compatibility of hardware and software;
- what data will be processed by the microcomputer system;
- how maintenance of equipment will be done; and
- the training needed for agency personnel.

Hardware and Software Inventories

We noted three of five agencies did not have complete or updated inventory listings of hardware and software. As a result we were unable to determine all the hardware and software owned by these agencies.

Adequate inventory systems provide additional security and control over the state's investment in microcomputers. Failure to maintain an adequate inventory system increases the potential for microcomputer equipment and peripherals to be misplaced, lost or stolen. Agencies should identify each piece of hardware and document: the location of equipment, the software installed, the responsible users, and an inventory of specific applications used on the system.

Similarly, it is important to develop an inventory of applications. An up-to-date inventory of applications helps assure employees are not developing similar applications and duplicating their efforts.

Training

In three of the five agencies reviewed we found training received by employees was inadequate. We noted some agencies had software applications installed on machines for employee use, but employees were unable to use them because employees were not properly trained.

Each agency should establish and maintain a minimum level of training for microcomputer users. All users should be trained to use all hardware and software specific to their job functions. Proper training would improve productivity and help eliminate unintentional mistakes caused by insufficient training.

Currently, agency personnel are receiving training in three ways. The primary source of training is being done through classes offered by the Information Services Division. Some personnel have taken advantage of classes offered by Vocational Technical Centers. Others rely on employees who are familiar with microcomputers and applications to provide cross-training.

Maintenance

The maintenance of microcomputers ranges from daily upkeep (cleaning, dusting, etc.), to the actual repair of microcomputers. Maintenance plans vary among agencies. Some provide their own maintenance of machines. Others rely on ISD for limited support; while others have maintenance contracts.

During our audit we found types of maintenance varied between bureaus and divisions within departments. There appeared to be little planning as to the method of maintenance to be used. We did not review maintenance programs for microcomputers on an individual basis; however, there are indications maintenance contracts as a standard practice may not be cost-effective. The majority of agencies chose to repair microcomputer equipment when there is a break down, rather than rely on maintenance contracts. Several agencies dropped maintenance contracts because of their expense. Maintenance contracts range from \$87 to \$373 per machine per year depending on the age and model of machine. This does not include costs for printer maintenance. The State of Kansas recently determined the average annual cost of a microcomputer maintenance contract is much higher than the actual cost of maintenance services on an as needed basis.

The type of maintenance to be provided for a microcomputer should be determined prior to purchase as part of overall needs (cost/benefit) analyses. Agencies need to determine how critical the microcomputer and its applications are to operations and the total data network. Maintenance plans then must be established accordingly.

Data Processing Personnel

With the arrival of micro-to-mainframe communication the microcomputer is more than a "personal computer." The involvement of mainframe computer processing with microcomputers makes it increasingly important agency data processing personnel are involved in the microcomputer acquisition and installation process. Once microcomputers are allowed to access mainframe computer data the issue of security over information becomes a greater concern. Data stored on the mainframe is subject to an Access Control Facility (ACF2) password protection application. When information is downloaded to a microcomputer this protection is lost and security becomes the responsibility of the user.

Section 2-15-114, MCA, provides, "each department head....shall designate an information security manager to administer the department's security program for data and information technology resources." Because state agencies are beginning to use microcomputers as substitutes for mainframes and to transfer information, the security manager's involvement in microcomputer system planning and operations is important.

We found two of the five agencies we reviewed had not included data processing personnel in plans to exchange information between the mainframe and microcomputers.

Conclusion

The Information Services Division should establish guidelines for organizational controls. These guidelines could be used by agencies in the formulation of policies and procedures that would establish effective microcomputer controls.

We found four of the five agencies we reviewed did not have adequate policies and procedures for microcomputers. Such policies and procedures help assure proper and consistent department planning and control of microcomputer usage. Policies will guide thinking and action in microcomputer operations. Procedures will establish customary methods of handling microcomputer equipment, peripherals and software.

RECOMMENDATION #1

WE RECOMMEND THE INFORMATION SERVICES DIVISION :

- A. DEVELOP MICROCOMPUTER GUIDELINES TO BE USED BY AGENCIES IN FORMULATING POLICIES AND PROCEDURES FOR EFFECTIVE ORGANIZATIONAL CONTROLS.
- B. DEVELOP MICROCOMPUTER GUIDELINES FOR INVOLVEMENT OF AGENCY DATA PROCESSING PERSONNEL IN PLANNING FOR THE ACQUISITION AND INSTALLATION OF MICROCOMPUTERS.

ACCESS AND SECURITY CONTROLS

During our audit we examined access and security controls existing over microcomputer hardware and software. Access should be controlled to provide adequate security over the microcomputer and peripherals. Appropriate access and security controls will ensure the accuracy and integrity of an agency's data. Section 2-17-503, MCA, provides "the Department of Administration is responsible for providing centralized management and coordination of state policies for security of data and information technology resources and shall establish and maintain the minimum security standards and policies to implement section 2-15-114, MCA, including the physical security of central and backup computer facilities consistent with these standards."

Physical Access

All of the agencies we reviewed had adequate physical controls over microcomputers. All microcomputers were stored in secure areas prohibiting public access. However, controls over access to diskettes and systems software were weak. We noted the following examples:

- In all five agencies we found diskettes containing data files stored next to microcomputers.
- In two agencies we found systems software stored next to microcomputers.

It is common industry practice to protect diskettes and the information on them from theft, loss, misplacement and manipulation, by storing the diskettes in locked file cabinets away from microcomputers. Systems software

should also be stored in a locked file cabinet or vault in order to prevent loss of state resources.

Logical Access

Logical access controls prevent access to information stored on microcomputers and diskettes. We found two agencies store confidential information on their microcomputer hard drives without any controls to prevent unauthorized access.

Access to confidential data stored on diskettes or hard drives can be secured several ways. Passwords can be assigned to control access to microcomputers or files. In order to enter into a file, the user would need to know the appropriate password. Passwords should be changed on a periodic basis.

Another alternative is to code the data by using encryption. The contents of the file would only be accessible by users who had approved access IDs. Encryption approaches are advantageous when a microcomputer is shared by several users.

If equipment must be shared by several users and cannot be monitored at all times, then file security mechanisms should be considered. Users could elect to store all confidential information on floppy diskettes, rather than on the microcomputer's hard drive.

Backup and Disaster Recovery

During our audit work we reviewed the backup and recovery procedures used by agencies. Backup and recovery planning consists of those activities undertaken in anticipation of potential disastrous events.

We found inconsistencies in backup methods and disaster recovery plans. These plans varied among departments and even within departments. Some departments did not have any backup procedures, while others had backups but lacked offsite storage areas. Backup and recovery capabilities should be sufficient to restore files and applications when loss or damage to data occurs. Backup files should be made whenever a significant change is made to a file. Individuals storing critical information on diskettes should be creating at least two backups of a file, one for offsite storage. For files stored on the hard

drive of the microcomputer, backup of the entire hard drive should be done on a periodic basis.

Adequate backup and recovery plans should also include backup equipment options. In case of a disaster, agencies could use other agencies' equipment or they could obtain equipment from the equipment pool established by ISD.

Conclusion

Based on our audit work, it appears overall access controls and disaster recovery plans are weak. The Information Services Division should establish guidelines for such controls. These guidelines could be used by agencies in formulating effective access controls and in developing disaster recovery plans for microcomputer systems.

RECOMMENDATION #2

WE RECOMMEND THE INFORMATION SERVICES DIVISION DEVELOP GUIDELINES TO BE USED BY AGENCIES IN FORMULATING ACCESS CONTROLS AND IN DEVELOPING DISASTER RECOVERY PLANS FOR MICROCOMPUTER SYSTEMS.

DOCUMENTATION

Application controls are specific controls over microcomputer systems that ensure the accuracy and integrity of data. During our audit we did not do an in-depth review of all the applications in each agency. We did test several spreadsheet applications and found the information being produced was reliable. We did note, however, concerns with application documentation.

In all five agencies we found examples of inadequate documentation for microcomputer applications. In one agency an application could not be accessed during an employee's absence because of the lack of documentation for that application. According to 1-0232.15 MOMs, "It is the policy of the Department of Administration that all application specific software developed by or for state agencies include adequate documentation."

User documentation should exist in order to enhance communication between various users and departments. Adequate documentation will provide

uniform information analysis and accountability; thus providing proper control over the integrity of information. Failure to maintain adequate documentation will cause data to be misunderstood and possibly misused by its users.

Security considerations over microcomputer hardware and software should also be given to documentation. Confidential application documentation should be kept in locked file cabinets and made available only to authorized personnel.

RECOMMENDATION #3

WE RECOMMEND THE INFORMATION SERVICES DIVISION ESTABLISH GUIDELINES FOR AGENCIES TO USE IN DOCUMENTING MICROCOMPUTER APPLICATIONS.

SOFTWARE LICENSING AND OWNERSHIP

There are basically two ways in which agencies can obtain software. The first way is to acquire ready-made software directly from a vendor. Secondly, software may be developed internally by agency personnel. During our audit work we noted concerns with both methods that are discussed below.

Software Licensing Agreements

Most of the software used with microcomputers is purchased from vendors. In some cases the purchase of this software does not transfer ownership to agencies, it only gives the agency a license to use the software on a certain microcomputer.

We found three of the five agencies reviewed were violating licensing agreements. Copy protection codes on the software were broken, allowing the software to be illegally copied. Unauthorized copying of software is a violation of Copyright Laws. Under the U. S. Copyright Law, civil damages for illegally copied software can be \$50,000 or more, depending on the amount of loss to the publisher. Failure of employees to follow licensing agreements may subject the state to potential lawsuits. Software vendors have filed million dollar lawsuits against corporations who have copied software.

According to employees in those agencies where software had been copied, they were not fully aware of copyright regulations. Consequently,

department policies should be formulated which educate employees of the possible consequences of copying protected software.

Ownership Rights

In auditing the sampled agencies, we discovered none of the agencies had formal policies for ownership rights of in-house or contract developed software.

Without clear ownership policies in existence, agencies are placing themselves at risk. Employees terminating employment may take an application they have developed; causing short or even long term interruptions in daily operations. Policies should exist which stipulate all software developed by agency personnel or by contract personnel is state property.

RECOMMENDATION #4

WE RECOMMEND THE INFORMATION SERVICES DIVISION DEVELOP GUIDELINES FOR AGENCY POLICIES ON OWNERSHIP RIGHTS AND LICENSING AGREEMENTS FOR MICROCOMPUTER SOFTWARE.

SUMMARY

This report has discussed some of the issues relating to organizational controls, access and security controls, documentation, software licensing agreements and software ownership rights that should be addressed by agencies using or contemplating the use of microcomputers. The Montana Operations Manual provides agencies with guidelines for mainframe acquisition and use, however these guidelines are not specific enough to cover microcomputer use. The Information Services Division has developed some preliminary guidelines for microcomputer management. We believe the development of such guidelines will improve the use of microcomputers statewide. Once these guidelines have been finalized, it will be up to individual agencies to administer the microcomputer function. As the complexity of microcomputer systems increase so will the risks. Agencies will need to apply controls accordingly.

AGENCY RESPONSE

DEPARTMENT OF ADMINISTRATION

DIRECTOR'S OFFICE



TED SCHWINDEN, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032

HELENA, MONTANA 59620

RECEIVED

MAR 10 1988

MONTANA LEGISLATIVE
AUDITOR

March 9, 1988

Jim Pellegrini
Deputy Legislative Auditor
Office of the Legislative Auditor
Room 135, State Capitol
Helena, MT 59620

Dear Jim:

Enclosed is our response to the recommendations in your audit regarding microcomputer use and control in state government.

If you have any questions please call.

Sincerely,

A handwritten signature in cursive script, appearing to read "Ellen Feaver".

Ellen Feaver
Director

Enclosure

RECOMMENDATION #1

WE RECOMMEND THE INFORMATION SERVICES DIVISION:

- A. DEVELOP MICROCOMPUTER GUIDELINES TO BE USED BY AGENCIES IN FORMULATING POLICIES AND PROCEDURES FOR EFFECTIVE ORGANIZATIONAL CONTROLS.
- B. DEVELOP MICROCOMPUTER GUIDELINES FOR INVOLVEMENT OF AGENCY DATA PROCESSING PERSONNEL IN PLANNING FOR THE ACQUISITION AND INSTALLATION OF MICROCOMPUTERS.

RESPONSE

The Department concurs with Recommendations A and B. The Department will address this problem in three ways: First, by updating topics currently covered in MOM to be specifically applicable to all classes of computers, not just mainframes. This update will be done by July 1, 1988; Second, by developing a model policy for Departments to use in preparing their own organizationally specific control and acquisition review policies. The Department will include the Data Processing Advisory Council and the Data Processing Managers group in the review of this model. This part will be done by December 31, 1988; Third, by covering the topics of microcomputer support, maintenance and training in the microcomputer management guidelines mentioned in your report. These will be finalized by July 1, 1988.

RECOMMENDATION #2

WE RECOMMEND THE INFORMATION SERVICES DIVISION DEVELOP GUIDELINES TO BE USED BY AGENCIES IN FORMULATING ACCESS CONTROLS AND IN DEVELOPING DISASTER RECOVERY PLANS FOR MICROCOMPUTER SYSTEMS.

RESPONSE

The Department concurs with the recommendation. The Department will address this recommendation by finalizing the draft microcomputer management guidelines mentioned earlier. The Department has contracted with the Big 8 accounting firm of Deloitte, Haskins, and Sells to consult with us and provide direction on computer security and disaster recovery. As part of that contract, they will assist us in writing those portions of the Microcomputer Management Guidelines. That contract will be complete and the guidelines finalized by July 1, 1988.

RECOMMENDATION #3

WE RECOMMEND THE INFORMATION SERVICES DIVISION ESTABLISH GUIDELINES FOR AGENCIES TO USE IN DOCUMENTING MICROCOMPUTER APPLICATIONS.

RESPONSE

The Department concurs with the recommendation. The Department will address this recommendation in the Microcomputer Management Guidelines by July 1, 1988.

RECOMMENDATION #4

WE RECOMMEND THE INFORMATION SERVICES DIVISION DEVELOP GUIDELINES FOR AGENCY POLICIES ON OWNERSHIP RIGHTS AND LICENSING AGREEMENTS FOR MICROCOMPUTER SOFTWARE.

RESPONSE

The Department concurs with the recommendation. The Department will address this recommendation in the Microcomputer Management Guidelines by July 1, 1988.

